



Positionspapier zur Novelle des Polizeigesetzes in Schleswig-Holstein

LAG Medien & Netzpolitik

TOPs

TL;DR.....	1
Einleitung.....	2
KI-gestützte Videoüberwachung.....	2
Automatisierte Datenanalyse.....	3
Fazit.....	5

TL;DR

Die geplante Novelle des Landesverwaltungsgesetzes (LVwG, im weiteren Verlauf „Polizeigesetz“ genannt), mit dem die Gefahrenabwehr für die Polizei geregelt wird (Drucksache 20/4284), ebnet den Weg in den Überwachungsstaat. Das CDU-geführte Innenministerium bedient sich dabei eines gefühlten Unsicherheitsempfindens um Grundrechte auszuhebeln. Wir fordern: Schluss mit dem Aktionismus. Wir brauchen eine Politik, die vernünftige und verfassungskonforme Lösungen schafft.

Zentrale Kernforderungen

- **Keine KI-gestützte Videoüberwachung:** Fehleranfällige Systeme entscheiden über polizeiliche Maßnahmen. Das untergräbt das Vertrauen in den Rechtsstaat.
- **Keine automatisierte Datenanalyse:** Massenüberwachung durch Social-Media-Daten greift in die informationelle Selbstbestimmung ein und schafft Diskriminierungsrisiken.
- **Modernisierung der Polizeiarbeit:** Investitionen in moderne Infrastruktur und länderübergreifende Zusammenarbeit sind vernünftige und verfassungskonforme Lösungen.



Echte Reformen statt Aktionismus

Die Polizeinovelle öffnet Pandoras Büchse. Einmal eingeführt, lässt sich Massenüberwachung nicht mehr zurückdrehen. Wir brauchen stattdessen Investitionen in moderne digitale Infrastruktur, die Grundrechte schützt und Sicherheit gewährt. Die Novelle hingegen schafft neue Risiken; autoritäre Strukturen, Missbrauchspotenzial und Kostenfallen. Die eigentlichen Probleme werden dabei nicht gelöst.

Einleitung

Schleswig-Holstein steht am Scheideweg: Geben wir ein großes Stück Freiheit für gefühlte Sicherheit auf? Öffnen wir die Tür zur Massenüberwachung? Überlassen wir Maschinen die Entscheidung, gegen wen Maßnahmen ergriffen werden?

Die Landesarbeitsgemeinschaft Medien & Netzpolitik von BÜNDNIS 90/DIE GRÜNEN in Schleswig-Holstein lehnt große Teile der geplanten Novelle des Polizeigesetzes ab. Die geplanten Änderungen basieren auf emotionalisierten Hypothesen und ebnen den Weg in einen Überwachungsstaat.

Wir Grüne stehen für Datenschutz. Es gibt viele gute Gründe, die persönlichen Daten unserer Bürger:innen zu schützen. Der Gesetzesentwurf will diesen Grundsatz brechen. Durch das Gesetz würden zwangsweise Daten erhoben, zusammengeführt und verarbeitet werden, die in keinem Zusammenhang mit der Gefahrenabwehr stehen. Insbesondere Anzeigende und Zeug:innen würden davon abgeschreckt werden.

Doch während Schleswig-Holstein objektiv sicherer wird (16,2% Rückgang der Straftaten im letzten Jahr)¹ rechtfertigt das Innenministerium die Novelle mit einem gefühlten Sicherheitsbedürfnis—ein Gefühl, das von Populisten propagiert wird, um die Gesellschaft zu spalten. Befürworter argumentieren, die Polizei bräuchte mehr Kompetenzen. Doch wo sind die Belege? Insbesondere das Attentat von Brokstedt ist aufgrund einer Fehlerkette möglich geworden. Eine Kamera hätte weder die Straftat verhindert, noch die Opfer geschützt.

Wir erkennen an: Die Polizei ist technisch nicht gewappnet. Doch aktionistischer Einsatz künstlicher Intelligenz und Massenüberwachung sind nicht die Lösung. Sie verschleiern nur die zugrundeliegenden Probleme.

1 <https://sh-gruene-fraktion.de/in-schleswig-holstein-lebt-es-sich-sicher/>

KI-gestützte Videoüberwachung

Videoüberwachung in Schleswig-Holstein ist auch an Orten erlaubt, an denen „Ordnungswidrigkeiten von erheblicher Bedeutung“ erwartet werden. Ein vager Begriff, der willkürlichen Einsatz ermöglicht. Ohne klare Kriterien kann die Videoüberwachung nach politischen Belieben installiert werden.

Die Überwachungskameras sollen mit KI-gestützten Verhaltensscannern ausgestattet werden. Künstliche Intelligenz erkennt nur Muster. Diese Muster sind weder nachvollziehbar noch enthalten sie notwendigen Kontext. So kann sie aus einer lebhaften Diskussion eine Schlägerei machen oder aus einem Handy ein Messer. Eine fehleranfällige, intransparente Überwachung ist nicht zufriedenstellend, um als Verbrechenserkenner der Polizei zu fungieren.

Kritisch sehen wir auch, dass für die KI-gestützte Fernidentifizierung massenhaft Referenzdaten aus Videoüberwachung und dem Internet gewonnen und verarbeitet werden sollen. Zudem wird die Kategorie „gefährdeter Orte“ eingeführt – ein Türöffner für flächendeckende Überwachung in Versorgungs- und Verkehrseinrichtungen.

Der Überwachungsausbau birgt erhebliches Missbrauchspotenzial. In Bayern nutzte die Regierung das dortige Polizeigesetz bereits, um die „Letzte Generation“ zu bekämpfen. Eine antidemokratische Regierung würde das Gesetz gezielt gegen politische Gegner ausnutzen. Dabei muss nicht einmal die Demonstration überwacht werden. Die Demonstranten können zuvor bereits über die Verkehrswege (gefährdete Orte) erfasst werden. Wer heute noch protestiert, steht morgen vielleicht auf einer Überwachungsliste.

Videoüberwachung führt zur Selbstzensur. Sie hat einen Einschüchterungseffekt. Die Sorge verdächtigt zu werden schränkt Betroffene in ihrer Meinungsfreiheit ein und schreckt vor Zivilcourage ab. KI-gestützte Videoüberwachung schafft durch ständige Beobachtung eine gläserne Öffentlichkeit, in der sich niemand mehr traut, sich frei zu bewegen.

„Social Sorting“ durch Menschen vermeiden zu können, ist ein scheinheiliger Vorwand. KI-gestützte Überwachung beugt Diskriminierung nicht vor, sondern webt sie in den Prozess ein, indem sie z.B. Kleidungsstücke als Verdachtsmoment einbezieht. Wer in Aussehen oder Verhalten von der KI-definierten Norm abweicht (z.B. weil ein Mensch einen Fan-Schal oder einen langen Bart trägt oder sich ungewöhnlich bewegt), wird verdächtiger eingestuft.

Die ausufernde Videoüberwachung im öffentlichen Raum lehnen wir ab. Sie macht es freien, unschuldigen Menschen unmöglich, sich privat im öffentlichen Raum zu bewegen. Wir weisen zudem darauf hin, dass der Ausbau flächendeckender Überwachung erhebliches Missbrauchspotenzial birgt.

Automatisierte Datenanalyse

Ziel der automatisierten Datenanalyse ist es, „anhand bestimmter Suchkriterien Personen zu identifizieren, die für eine Gefahrenlage verantwortlich sind“. Der Entwurf schließt die Nutzung von selbstlernenden Systemen zwar aus, die Beständigkeit dieser Beschränkung ist jedoch flüchtig. Durch die einfache Streichung eines Passus kann sie aufgehoben werden. Referenzen auf den AI Act sind weitere Indizien für die geplante Nutzung von KI, die das CDU-geführte Innenministerium anscheinend vorsieht. Eine Weiterentwicklung des Automatisierungsgrades, wie es eine Streichung der Restriktion ermöglichen würde, lehnen wir ab. Jeder Schritt in die Richtung Predictive Policing ist einer zu viel.

Der Gesetzesentwurf ermöglicht der Polizei sämtliche personenbezogenen Daten automatisiert zu verarbeiten – auch Daten von Databrokern oder aus den sozialen Medien. Die Datenhoheit legt das Gesetz aber nicht fest. Neben fragwürdiger Vereinbarkeit mit EU-Recht, stellt diese Form des Datenkaufs einen der gravierendsten Eingriffe in die informationelle Selbstbestimmung dar. Sensibelste, lebenslang im Internet beständige Daten werden gespeichert und können jederzeit gegen den Bürger verwendet werden. Niemand kontrolliert, ob diese Daten überhaupt korrekt sind.

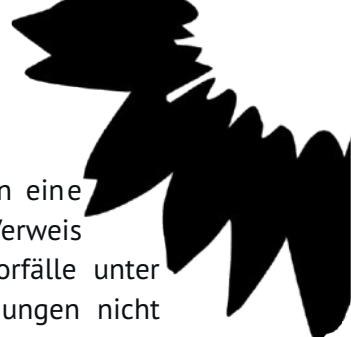
Bereits die Nutzung dieser Daten ist besorgniserregend. Obendrein besteht aber auch die realistische Gefahr, einer missverständlichen, falschen oder sogar gefälschten Zuordnung und Verknüpfung. Im Anschluss sollen diese Daten fragwürdiger Legitimität zur biometrischen Fernidentifizierung verwendet werden dürfen. Auch der Europäische Datenschutzausschuss (EDSA) stellt infrage, ob vergleichbare Maßnahmen mit EU-Recht vereinbar sind. Biometrische Fernidentifizierung in öffentlichen Räumen ist eine Form der Massenüberwachung, die Demokratien grundsätzlich fernliegen sollte.

Die automatisch generierten Profile kann niemand nachvollziehen. Niemand kann vollständig nachvollziehen, welche Informationen überhaupt richtig sind, ob die Zusammenhänge stimmen oder wer sie verfälscht hat. Das ist keine verantwortungsvolle Basis für Rechtsstaatlichkeit.

Durch Identitätsdiebstahl könnten Kriminelle, wie Stalker:innen oder Betrügerbanden, Opfer polizeilich diskreditieren. Erpressung und psychologischer Terror können die Folgen sein. Der Staat ist selbst nicht in der Lage, die Daten seiner Bürger:innen zu schützen, wie es gerade in Berlin zu sehen ist.

KI-Systeme reproduzieren Vorurteile. Vorurteile, die einen Menschen verdächtig erscheinen lassen, obwohl er es nicht ist, was insbesondere Minderheiten und deren soziales Umfeld kriminalisiert. Menschen trauen sich nicht mehr, ihre Meinung frei zu äußern aus Angst, später in den Fokus der Polizei zu geraten. Wer damit rechnen muss, in einer Datenanalyse zu landen, wird zögern, Anzeigen zu erstatten oder sich als Zeuge zu melden. Dieser sogenannte Chilling-Effekt treibt zur Selbstzensur und erschüttert das Vertrauen in unsere Demokratie.

Während wir künstliche Intelligenz in anderen Bereichen (z.B. autonomes Fahren) aus gutem Grund ausschließen, soll unausgereifte Technologie hier in hochsensiblen Bereichen eingesetzt werden. KI ist fehleranfällig, intransparent und „halluziniert“. Sie ist kein intelligentes System, sie fußt auf Wahrscheinlichkeiten, ohne wichtigen Kontext zu verstehen. Das kann auch dazu führen, dass relevante Fakten ignoriert werden.



Wer ist verantwortlich für die zerstörten Existenzen, wenn Entscheidungen an eine Entscheidungsmaschine ausgelagert werden? Diese Frage ist essenziell, denn der Verweis auf den „Human in the Loop“ ist eine gefährliche Illusion. Beamte müssen Vorfälle unter wachsendem Zeitdruck bewerten und können die intransparenten KI-Entscheidungen nicht nachvollziehen. Am Ende trifft es uns alle, wenn wir uns nicht an die KI-normierten Verhaltensmuster anpassen. Gerade im Bereich der digitalen Ethik wünschen wir uns mehr Sensibilität.

Anstatt die Löcher im Fundament zu reparieren, versucht die Landesregierung sie mit Aktionismus zu stopfen. Anstelle einer kohärenten Datenstrategie werden teure, unausgereifte KI-Systeme auf zerstreute Daten losgelassen. Das ist nicht nur technischer Humbug, sondern kann sich rasch als Kostenfalle entpuppen. In Zeiten knapper Kassen ist das besonders unverantwortlich.

Fazit

Die LAG Medien & Netzpolitik fordert stattdessen, dass Behörden ihre Hausaufgaben machen, ihre Daten entsprechend einer modernen Datenstrategie aufbereiten und die länderübergreifende Kommunikation endlich modernisieren.

In einem freiheitlich-demokratischen Land wie der Bundesrepublik Deutschland ist der verantwortungsvolle Umgang beim Sammeln und Speichern von Daten das oberste Gebot. Daher sind Begehrlichkeiten wie die anlasslose Erfassung von Massendaten grundsätzlich abzulehnen. Auch im öffentlichen Raum darf der Bürger nicht unter Generalverdacht gestellt werden.

Ist Pandoras Büchse erst einmal geöffnet, lässt sie sich nicht mehr schließen. Es hilft nicht, mehr Technik über Probleme zu stülpen. Die Probleme liegen an der Wurzel. Die Fachverfahren und die behördenübergreifende Kommunikation sind mangelhaft – mehr Befugnisse sind keine Lösung. Je länger die Löcher im Fundament ignoriert werden, desto teurer wird eine unvermeidliche Reform dieser Strukturen.

Einer möglichen antidemokratischen Regierung würden solche Instrumente ermöglichen, autoritäre Strukturen, ohne Kenntnis der Öffentlichkeit und parlamentarischer Opposition, zu etablieren. Aber auch für das demokratische System ist es ein Problem, wenn Regierungen sich immer autoritärer Mittel bedienen, statt Lösungen für die Ursachen zu suchen und diese askömmlich zu finanzieren.

BÜNDNIS 90/DIE GRÜNEN trägt eine besondere historische Verantwortung für die Zivilgesellschaft. In einer Demokratie muss der Staat dem Bürger vertrauen!

Kiel, den 11.09.2026

LAG Medien & Netzpolitik